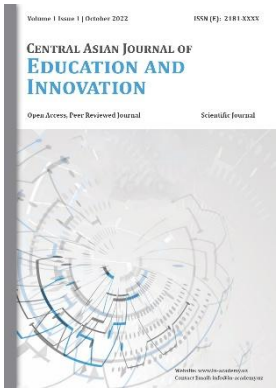

FIRIBGARLIK SHAKLIDA SODIR ETILGAN KIBERJINOYATLAR

Tashtanboyev Ro‘zimat Tolib o‘g‘li
Jamoat xavfsizligi universiteti 1-kurs magistratura talabasi
https://doi.org/10.5281/zenodo.17964612

ARTICLE INFO

Qabul qilindi: 10-dekabr 2025 yil
Ma’qullandi: 14-dekabr 2025 yil
Nashr qilindi: 17-dekabr 2025 yil

KEY WORDS

aqamli texnologiyalar, raqamli transformatsiya, kiberjinoyat, kiberfiribgarlik, axborot xavfsizligi, internet jinoyatlari, kompyuter tarmoqlari, onlayn to‘lov firibgarligi, bank tizimi xavfsizligi, raqamli savodxonlik, kiberxavfsizlik, axborotlashtirish, elektron tijorat, konvensiya, xalqaro hamkorlik, kiberxavfsizlik siyosati, huquqiy islohotlar, texnologik choralar, sun’iy intellekt, ma’lumotlarni himoya qilish, fuqarolar xavfsizligi..

ABSTRACT

Ushbu maqola raqamli texnologiyalar rivoji va uning jamiyat hayotiga, xususan kiberjinoyatlar va kiberfiribgarlikka ta’siri muammosini yoritadi. Maqolada kiberjinoyat va kiberfiribgarlik tushunchalari hamda ularning global va O‘zbekiston kontekstidagi tarqalishi, statistik ko‘rsatkichlari, asosiy texnik va psixologik usullari tahlil qilinadi. Shuningdek, qonuniy bazasi va xalqaro hamkorlik zaruriyati ta’kidlanadi. Muammoni hal etish uchun huquqiy islohotlar, milliy kiberxavfsizlik siyosati, raqamli savodxonlikni oshirish, texnologik choralar va tashkilot ichki siyosatlari taklif etilgan. Xulosa sifatida — integratsiyalashgan choralar amalga oshirilsa, kiberfiribgarlik darajasi sezilarli kamayishi ta’kidlanadi.

Kiberjinoyat O‘zbekistonda eng jiddiy tahdidlardan biri bo‘lib qolmoqda — ro‘yxatga olingan jinoyatlarning 42 foizi unga to‘g‘ri keladi. Prezidentimiz ushbu turdagi jinoyatlarga qarshi kurashishni va infratuzilmani rivojlantirishni chora-tadbirlarini ishlab chiqishni topshirdi.

2025-y. 9-iyul. O‘zbekiston Respublikasi prizidenti Sh.M.Mirziyoyev

Bugungi kunda raqamli texnologiyalar jadal sur’atlarda rivojlanib, hayotimizning deyarli barcha jabhalariga kirib kelmoqda. Yangi turdagi innovatsion texnologiyalar yaratilishi natijasida inson aralashuvisiz bajariladigan ishlar soni ortib, mehnat jarayonlari avtomatlashtirilmoqda. Shu bois raqamli transformatsiya nafaqat ishlab chiqarish, balki ta’lim, tibbiyot, moliya va kundalik turmush tarzimizni ham tubdan o‘zgartirmoqda. Barcha sohalarda buni samarali va foydali taraflar juda ko‘p bo‘lishiga qaramasdan salbiy oqibatlari ham yo‘q emas. Bu masalani ham imkon qadar bartaraf etilishga qadam va qadam erishilmoqda. Ushbu muammolardan biriga to‘xtaladigan bo‘lsak, texnalogiyalar orqali jinoat olamida fribgarlik shaklida sodir etilayotgan jinoyatlar soni oshib bormoqda. Ushbu jinoyatlarni oldini olish va

bartaraf etish harakatlari olib borilishiga qaramasdan, jinoyatchilar ya'ni kiberjinoyatchilar, kiberfribgarlar ham boshqa usullarni, yangi usullarni o'ylab topishdan hech charchashmayotgani hammaizga ma'lum. So'ngi yillarda butun dunyoda raqamli texnalogiyalar bilan, kampuyter texnalogiyalari bilan sodir etilgan fribgarlik soni otib bormoqda. Bu jarayonlar salkam 50 yil oldin boshlangan. Bu jarayon raqamli texnalogiyalar rivojlangani sari kiberfribgarlik ham baravar rivojlanib bormoqda. Ushbu jinoyatlar bugungi kunda O'zbekistonni ham chetlab o'tmadi. Bizni yurtimizda ham raqamlashtrish siyosati ketayotgan bir paytda kiber tahdidlardan himoyalanishni ham zamon talab qilmoqda. Shuningdek, aynan kiberxvfsizlik statistikasiga qaraydigan bo'lsak, raqamli texnalogiyalar orqali 2025-yil oxirigacha dunyo 10.29trln dollar zarar ko'rishi pragnoz qilinmoqda. O'zbekistonda esa o'tgan yilgi statistikaga qaraydigan bo'lsak, 2024-yil 58 800ta kiberjinoyat, bundan 97,7%i bank tarmoqlariga to'g'ri keladi. Ushbu masalani o'rganishning ahamiyati shundaki **zamonaviy raqamli muhitda yuzaga kelayotgan yangi turdagi jinoyatlarni chuqur tahlil qilish, ularning sabablari, usullari va oqibatlarini aniqlash** hamda **ularni oldini olish bo'yicha samarali chora-tadbirlar ishlab chiqish**dir. Bunda Iqtisodiy, huquqiy, ijtimoiy va taxnalogik ahamiyat mavjud.

Kiberjinoyat — bu kompyuter tarmoqlari, internet, mobil aloqa yoki boshqa raqamli vositalardan foydalangan holda sodir etiladigan har qanday noqonuniy harakatlarni anglatadi. Bunday hujumlar ko'pincha ma'lumotlarni o'g'irlash, buzish yoki tarqatish, shaxsiy ma'lumotlardan noqonuniy foydalanish yoki moliyaviy foyda ko'zlash kabi maqsadlarni ko'zlaydi. Axborot va kommunikatsiya texnologiyalarining tez rivojlanishi kiberjinoyatlarning tarqalishini kuchaytirmoqda va ular hayotning deyarli barcha sohalariga ta'sir etmoqda. Kiberjinoyatlar orasida eng tarqalgan turlaridan biri — firibgarlikdir. Kiberfiribgarlikda jinoyatchilar odamlarning ishonchidan foydalanib, ularni aldash orqali pul yoki muhim ma'lumotlarni qo'lga kiritishga harakat qiladi. Masalan, soxta onlayn-do'konlar orqali xaridorlardan pulni talab qilish, soxta xabarlar (phishing) yuborish yoki bank kartalarining ma'lumotlarini o'g'irlash — bularning barchasi kiberfiribgarlik misollaridir. Shu sababli bu turdagi jinoyatlar axborot xavfsizligida jiddiy muammo hisoblanadi. An'anaviy firibgarlik va kiberfiribgarlik o'rtasida muhim farqlar bor. An'anaviy holatlarda jinoyatchi jabrlanuvchi bilan ko'proq yuzma-yuz yoki cheklangan hudud doirasida muloqot qiladi, holat mahalliy xususiyatga ega bo'ladi. Kiberfiribgarlik esa internet orqali amalga oshirilgani uchun jinoyatchining kimligi ko'pincha sirligicha qoladi va hujumlar geografik chegaralarsiz — global miqyosda sodir bo'lishi mumkin. Bunda texnik vositalar (masalan, zararli dasturlar) va psixologik usullar (masalan, ishonchni suiiste'mol qilish) birgalikda qo'llanadi — soxta saytlar yoki ijtimoiy tarmoqlar orqali odamlarni aldash keng tarqalgan usullardir.

O'zbekistonda kiberjinoyatlar, jumladan, kiberfiribgarliklarni tartibga soluvchi qator qonuniy asoslar mavjud. Eng avvalo, **O'zbekiston Respublikasi Jinoyat kodeksi**da bu masalaga oid normalar aniq belgilangan. Xususan, **168-modda** firibgarlik uchun, **278^1-278^7-moddalar** esa kompyuter axborotiga noqonuniy kirish, undan ruxsatsiz foydalanish va kompyuter tizimining ishlashini buzish uchun javobgarlikni belgilaydi. Shuningdek, "**Axborotlashtirish to'g'risida**"gi qonun, "**Elektron tijorat to'g'risida**"gi qonun, xalqaro miqyosda esa **Budapesht konvensiyasi** (2001-yil) kiberjinoyatlarga qarshi kurashda asosiy hujjat sanaladi. Ushbu konvensiya davlatlar o'rtasida hamkorlikni yo'lga qo'yish, tergov jarayonlarini muvofiqlashtirish hamda jinoyatchilarni aniqlash va jazolash tartibini belgilaydi.

Shuningdek, **Interpol** va **BMT Giyohvandlik va jinoyatchilik boshqarmasi (UNODC)** tomonidan ham kiberjinoyatlarga qarshi xalqaro tavsiyalar ishlab chiqilgan.

Kiberfiribgarlik — bu raqamli muhitda foydalanuvchilarni aldash, ularning shaxsiy yoki moliyaviy ma'lumotlarini noqonuniy yo'l bilan qo'lga kiritish, shuningdek, moddiy zarar yetkazish maqsadida amalga oshiriladigan noqonuniy harakatlardir. Amaliyotda uchraydigan kiberfiribgarlik turlarining eng keng tarqalgan shakllariga quyidagilar kiradi: **fishing** (soxta elektron xabarlar orqali foydalanuvchini aldash), **social engineering** (inson psixologiyasidan foydalanib ma'lumot olish), **onlayn to'lov firibgarligi** (soxta saytlar orqali to'lovlarni o'g'irlash), **bank kartasi ma'lumotlarini o'g'irlash**, **soxta investitsiya va kriptovalyuta loyihalari**, shuningdek, **mobil ilovalar orqali amalga oshiriladigan aldov sxemalari**. Bunday usullar yordamida jinoyatchilar foydalanuvchilarning e'tiborini chalg'itish yoki ishonchini qozonish orqali ularning moliyaviy resurslarini egallab olishadi.

Kiberfiribgarlik oqibatida fuqarolar va tashkilotlar turli yo'nalishlarda zarar ko'rishadi. Avvalo, **moliyaviy yo'qotishlar** eng ko'p uchraydigan zarar turi hisoblanadi — bu bank kartalaridan noqonuniy yechimlar, to'lov tizimlarida mablag'larning o'g'irlanishi yoki firibgarlik orqali investitsiya yo'qotishlarida namoyon bo'ladi. Shu bilan birga, **shaxsiy ma'lumotlarning oshkor bo'lishi, obro'-e'tiborga putur yetishi, axborot tizimlarining ishlashining izdan chiqishi** va **ma'lumotlar bazasining buzilishi** kabi holatlar ham keng tarqalgan. Tashkilotlar uchun esa bu jarayon nafaqat moliyaviy zarar, balki ishonchni yo'qotish va mijozlar bilan munosabatlarning yomonlashishiga olib keladi.

Bunday jinoyatlarni aniqlash va oldini olishda bir qator muammolar mavjud. Eng avvalo, kiberjinoyatlar **anonim tarzda**, ya'ni jinoyatchining shaxsini aniqlash qiyin bo'lgan muhitda amalga oshiriladi. Shuningdek, **texnik izlarni yashirish**, **VPN yoki dark web** kabi vositalardan foydalanish, **transchegaraviy xususiyat** — ya'ni jinoyat bir davlatda sodir etilib, zarari boshqa davlatda yetkazilishi — tergov jarayonini murakkablashtiradi. Fuqarolarning axborot savodxonligi pastligi ham kiberfiribgarlikka qarshi kurashda muhim to'siq bo'lib qolmoqda.

Kiberfiribgarlikka qarshi samarali kurash — bu faqat texnik vositalarga emas, balki keng qamrovli huquqiy, ijtimoiy va tashkiliy choralarni talab etadigan kompleks jarayondir. Avvalo davlat darajasida kiberxavfsizlik siyosatini yangilash va unga qat'iy operatsion mexanizmlar joriy etish zarur. Shu ma'noda, jinoyat kodeksi va tegishli normativ hujjatlarni zamonaviy kiberjinoyat shakllarini qamrab oladigan tarzda yangilash, mazkur hodisalar bo'yicha majburiy xabar berish mexanizmini qonuniylashtirish hamda kritikal infratuzilmalar uchun muntazam kiberxavfsizlik auditi va sertifikatlashtirishni joriy etish ustuvor vazifalardir. Ushbu huquqiy tartib-intizom jinoyatlarni aniqlash, tergov va sud bosqichida samaradorlikni oshirishga xizmat qiladi.

Ikkinchi muhim yo'nalish — fuqarolar va xodimlarning raqamli savodxonligini oshirishdir. Kiberfiribgarlikning katta qismi inson omilidan — e'tiborsizlik, ma'lumot yetishmasligi yoki ijtimoiy muhandislikka aldanishdan kelib chiqadi. Shu bois, maktabdan boshlab oliy ta'limgacha bo'lgan o'quv dasturlariga kiberxavfsizlik asoslarini kiritish, davlat va xususiy sektor hamkorligida milliy kampaniyalar o'tkazish, tashkilotlarda muntazam treninglar tashkil etish zarur. Jabrlanganlarga tez texnik va huquqiy yordam ko'rsatish uchun 24/7 maslahat xizmatlari va onlayn qo'llanmalar tashkil etilishi ham muhim ahamiyatga ega. Texnologik choralar kiberfiribgarlikni aniqlash va oldini olishda markaziy o'rin tutadi. Barcha onlayn xizmatlar va moliya tashkilotlari uchun ikki bosqichli yoki ko'p bosqichli shaxsni

aniqlash tizimini majburiy qilish kerak. Korxonalar va muassasalar uchun Endpoint Detection & Response (EDR- **kompyuterlar, noutbuklar, telefonlar** kabi qurilmalarda sodir bo‘layotgan **xavfli harakatlarni kuzatib turuvchi va zarur bo‘lsa darhol javob beruvchi tizim**), Security Information and Event Management (SIEM - **tizimdagi barcha xavfsizlik hodisalarini bir joyda yig‘ib, tahlil qiluvchi markaziy dastur**) hamda Security Operations Center (SOC- axborot xavfsizligi bo‘yicha mutaxassislar ishlaydigan markaz) kabi infratuzilmalarni yo‘lga qo‘yish, shuningdek, sun’iy intellekt va mashina o‘rganish texnologiyalaridan foydalanib trafik va tranzaksiyalarni yondashuv asosida tahlil qilish orqali firibgarlik modellari avtomatik aniqlanadi va bloklanadi. Deepfake va ovoz-soxtalashtirish kabi yangi tahdidlarni aniqlash uchun media tekshiruvi va biometrik tekshiruvlar joriy etilishi lozim. Bularni natijalariga qaraydigan bo‘lsak, bugungi kunda NASA [7], FBI va shunga o‘xshagan katta-katta kompaniyalar o‘z tizimini maksimalni ximoya qilib kelmoqda.

Tashkiliy jihatdan har bir tashkilotda Incident Response Plan (IRP) bo‘lishi, rollar va javobgarliklar aniq belgilanishi kerak. Ichki siyosatlarda least-privilege tamoyilini (minimal ruxsatlar) qo‘llash, role-based access control (RBAC) joriy etish va yetkazib beruvchilar xavfsizligini baholash — supply-chain xatarlarini kamaytiradi. Ransomware hamda boshqa tahdidlar qarshi mustahkam backup va tiklash strategiyalari (isolated/off-site backup, RTO/RPO parametrlarini belgilash) ishlab chiqilishi kerak[8]. Xalqaro hamkorlik — transchegaraviy kiberjinoyatlar bilan kurashning ajralmas qismidir. Davlat va tashkilotlar o‘rtasida CERT/CSIRTlararo tezkor axborot almashish protokollari, Interpol va boshqa xalqaro tashkilotlar bilan ma’lumot almashish va tergov hamkorligini kuchaytirish zarur. Shuningdek, ma’lumotlarni hisobotlash va statistika standartlarini bir xillash orqali global tendensiyalarni aniqroq kuzatish mumkin bo‘ladi.

Yuqoridagi choralarni baholash va monitoring qilish uchun aniq indikatorlar (KPIs) belgilanishi muhim: fishing testlaridagi xodim muvaffaqiyati 85%, breach notificationga rioya qilish: 95% holat 72 soat ichida xabar berilishi, SOC yordamida tahdidni aniqlash va javob vaqti 1 soat kabi mezonlar samaradorlikni o‘lchashga yordam beradi.

Xulosa qilib aytganda, kiberfiribgarlikka qarshi kurash kompleks va uzluksiz jarayon bo‘lib, unda huquqiy islohotlar, jamiyatning raqamli savodxonligi, tashkilotlarning ichki siyosatlari va ilg‘or texnologik vositalarning uyg‘unligi muhim omillar hisoblanadi. Ushbu chora-tadbirlar mukammal va ketma-ket amalga oshirilsa, kiberfiribgarlik darajasi sezilarli darajada kamayadi, fuqarolar va tashkilotlar raqamli makonda yuqori darajada himoyalangan bo‘ladi.

Ushbu o‘rganilgan masalalar asosida shuni xulosa qilish mumkinki, kiberfiribgarlik zamonaviy jamiyat xavfsizligiga jiddiy tahdid solayotgan global muammo hisoblanadi. Kiberfiribgarlikka qarshi samarali kurash olib borish uchun davlat, fuqarolar va tashkilotlar o‘rtasida mustahkam hamkorlik zarur. Davlat organlari huquqiy bazani takomillashtirib, kiberxavfsizlik infratuzilmasini mustahkamlashi lozim. Tashkilotlar esa o‘z axborot tizimlarini himoya qilish, xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitish va xavf tahlilini olib borish orqali o‘z mas’uliyatini oshirishi kerak. Fuqarolar ham o‘z navbatida raqamli savodxonlik darajasini oshirishi, shaxsiy ma’lumotlarini himoya qilish, shubhali havolalar va noma’lum manbalarga ishonmaslik madaniyatini shakllantirishi zarur. Huquqshunaslar ushbu vaziyatlarni oldini olishga kerakli normalarni yaratib berishlari, ushbu amaliyotlarni qonuniy qo‘llanilishi uchun qonuniy asoslar yaratib berish kerak, kiberfribgarliklarni oldini olish uchun

barcha huquqiy harakatlar sodir etilishi kerak. Jinoyat sodir etilganidan so‘ng ham ularni aniqlash, dalillarni to‘plashda malakali kadirlarni ishga jalb qilib jinoyatni ochishda kerak bo‘ladigan barcha texnikaviy vositalar bilan taminlashizmiz kerak. Imkon qadar chet el tajribalarini, qounlarini, ushbu muammoni bartaraf etish usullarni O‘zbekistonda ham implementatsiya qilishimiz kerak hisoblanadi.

Foydalanilgan manbalar:

1.207 Cybersecurity Stats and Facts for 2025 https://www.vikingcloud.com/ (murojat sanasi 10.13.2025)

2.Ущерб от киберпреступлений в 2021–2024 годах в Узбекистане превысил 1,9 трлн сумов https://www.gazeta.uz (murojat sanasi 10.13.2025)

3.The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols https://www.coe.int/ (murojat sanasi 10.13.2025)

4.Uzbekistan sees 68-fold surge in cybercrime: Nearly 2 trillion UZS stolen in five years https://kun.uz (murojat sanasi 10.13.2025)

5.O‘zbekiston Respublikasining 1995- yil 22-sentabr kunidagi “O‘zbekiston Respublikasi Jinoyat kodeksi”. https://lex.uz (murojat sanasi 10.13.2025)

6.A Computer Emergency Response Team (CERT) https://www.group-ib.com (murojat sanasi 10.13.2025)

7.Data Science, Cyber, & IT // URL : https://www.nasa.gov/ (murojat sanasi: 14.12.2025)

8.Cloud Security Best Practices Every Organization Should Follow // URL : https://www.aikido.dev/ (murojat sanasi: 14.12.2025)